Hidden Markov Model Baseline for Flexible Assembly System Anomaly Detection - DRAFT

Tero Keski-Valkama

Version: January 2, 2022

***Abstract*—**

***Index Terms*—**

I. Introduction

Flexible Assembly Systems (FAS) and Flexible Manufacturing Systems (FMS) represent an evolution from specialized mass manufacturing systems. They allow flexibility in manufacturing which enables efficient production of smaller production runs and customization, personalization and quick evolution of manufactured products.

Flexibility brings challenges as it makes fault detection harder, especially in systemic conditions. Even if each separate module of a flexible assembly plant was nominally operating well, there are systemic fault modes and degradations which can cause non-optimal performance of the whole. Novel production plans deployed to the manufacturing system evokes new behaviours and possible problems. As flexible manufacturing generally requires more open integration to external systems for planning and controlling production dynamically, it becomes more susceptible to cyberattacks.

Many of these fault conditions and degradations are such that they cannot be trivially known in advance. Industrial anomaly detection systems are used to detect novel anomalous conditions which might denote faults, degradations or for example cyberattacks. Traditional process mining methods are not well suitable for environments with heterogeneous industrial IoT systems creating logs where process trace events might not be fully correlated with the process ids. These uncorrelated process traces or logs are therefore interlaced so that events are in sequence but originating from separate processes. In general case, automatic process identification might not be even possible in an explicit form.

Machine learning approaches can provide automatic learning of industrial process nominal operation, and those can be used to flag anomalous situations. Machine learning systems require data to train on, and industrial process data is guarded trade secret especially in relation to fault conditions. Real data on manufacturing process faults is nontrivial to get in sufficient amounts and on system level. Hence, simulations for synthetic flexible assembly process are required. In this research, FAS Simulator is used as the data source [1].

To compare different machine learning approaches, baselines are needed. We are interested in anomaly detection solutions for uncorrelated process traces, or sequential, interlaced event logs. Existing methods for these include Hidden Markov Model based approaches [2] [3], denoising autoencoder based approaches [4], LSTM based approaches [5] [6], or even more complex deep neural networks [7]. Some of the traditional approaches such as Alpha algorithm from process mining require correlated process traces, where each event is tagged with the process instance it belongs to, effectively deinterlacing the event logs.

Here we present results of applying Hidden Markov Models on FAS Simulator datasets to produce a baseline benchmark for this challenge to compare more sophisticated approaches against.

II. Setup

We generated challenge data using FAS Simulator project [8]. The challenge dataset consists of 10,000 runs of healthy flexible assembly system and 10,000 runs of a flexible assembly system under a randomly picked degrading condition. Each run consists of assembling 30 items, slightly over 1,000 events logged each.

The data is divided into training set of the first 90,000 healthy runs, and the validation set of the final 10,000 healthy runs and all the 100,000 degraded runs. For training, 1,000 runs are picked from the training set randomly, and for validation 1,000 runs are picked from the validation set randomly.

64 Hidden Markov Models are trained with different numbers of hidden states from 1 to 64. Different lengths of windows are used to train and evaluate the model, with window sequence lengths of 10, 100, 1,000 and full runs.

These models are used to score the overall likelihood of the observed sequence window assuming the trained model for the validation set sample sequences. In practice we find that the model tends to score sample sequences from the degraded runs higher in likelihood than from the healthy runs. This is likely due to the fact that HMM is unable to perfectly model the causal relationships in the process traces, and that degraded sequences tend to have a higher frequency of "TICK" events in the traces designating the passing of time. As "TICK" events are the most common event type in the training set as well, their respective probability is very high compared to other event types. This makes the HMM score degraded logs higher than healthy logs.

Other research using HMMs for anomaly detection has also found that naive scoring of the sequences doesn't work well for this purpose [2]. Instead, they tend to suggest looking at the HMM hidden state sequences and differences of those to the healthy hidden state sequences.

In our case, the event ids are static across sequences, and the trained HMM model is static as well, so we can simply compare the hidden state sequences directly without the added complication of equivalence or similarity of different Hidden

Markov Models. We simply compute histograms of hidden states in the observed window for the trained HMM, and compare the histograms to the histograms of the training set using KL divergence.

REFERENCES

[1] T. Keski-Valkama, "A simulator for event-oriented data in flexible assembly system fault prediction," *Procedia computer science*, vol. 119, pp. 121–130, 2017.

[2] N. Görnitz, M. Braun, and M. Kloft, "Hidden markov anomaly detection," in *International conference on machine learning*. PMLR, 2015, pp. 1833–1842.

[3] S. S. Joshi and V. V. Phoha, "Investigating hidden markov models capabilities in anomaly detection," in *Proceedings of the 43rd annual Southeast regional conference-Volume 1*, 2005, pp. 98–103.

[4] T. Nolle, A. Seeliger, and M. Mühlhäuser, "Unsupervised anomaly detection in noisy business process event logs using denoising autoencoders," in *International conference on discovery science*. Springer, 2016, pp. 442–456.

[5] L.-P. Yuan, P. Liu, and S. Zhu, "Recompose event sequences vs. predict next events: A novel anomaly detection approach for discrete event logs," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021, pp. 336–348.

[6] M. Du, F. Li, G. Zheng, and V. Srikumar, "Deeplog: Anomaly detection and diagnosis from system logs through deep learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1285–1298.

[7] X. Zhang, Y. Xu, Q. Lin, B. Qiao, H. Zhang, Y. Dang, C. Xie, X. Yang, Q. Cheng, Z. Li *et al.*, "Robust log-based anomaly detection on unstable log data," in *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, 2019, pp. 807–817.

[8] T. Keski-Valkama, "Flexible assembly simulation: FAS Simulator." [Online]. Available: https://github.com/keskival/FAS-Simulator

Tero Keski-Valkama Tero Keski-Valkama is working as a lead ML & AI engineer in HERE Switzerland GmbH. He has been programming neural networks since high school in 1990s.